Pentagon Likely To Outfit Common Access Cards With New Features

Inside The Pentagon, pg. 3
September 12, 2002

The Pentagon is looking to design new capabilities into its common access card, identification being issued to all Defense Department personnel. While only about a third of DOD employees currently carry the card, next-generation CACs could appear as soon as early 2003.

Officials say future features depend entirely upon what military installations require. Technology exists to outfit the card with almost anything, they said.

Accordingly, last month, Pentagon Chief Information Officer John Stenbit issued a "data call" to DOD bases and offices, requesting information on methods and technologies currently employed to restrict physical access.

"The physical security community has not necessarily closely managed what types of security systems have been deployed where," said Rob Carey, e-business and smart card policy lead for the Navy chief information officer. The Navy is leading CAC implementation.

DOD is looking for "who has what" and how many people are affected, he told reporters Sept. 10. Carey said a senior coordinating group will assess the responses this fall and hopefully pick a new CAC configuration by November.

"It helps us understand what kind of technology should get on this card," he said, adding that the goal is to "marry as much of the population that we can."

New CAC designs will not require personnel to trade out their existing cards. Because the cards typically have a three-year lifespan, Carey said he expects employees will be issued a new, updated CAC after their card expires.

The Defense Manpower Data Center issued the 1 millionth CAC at Ft. Belvoir, VA, last month. Officials anticipate approximately 3.5 million personnel will have cards by the end of 2003.

Most DOD identification badges are "flash and pass" cards. The CACs will eventually replace almost all badges, allowing employees both physical access to restricted buildings as well as access to computer networks. CACs provide digital certificates to authenticate and encrypt messages.

So far, some Navy officials are using the CACs to log on to their computers — a capability expected to spread as the CACs become more common and a cryptographic methodology is developed. Also, all Army general officers are currently using their cards to sign e-mails.

The CAC is regarded as a work in progress and relies heavily on the cooperation of individual bases and offices to integrate the technology into their security process, Carey said.

"There are a lot of processes and cultural changes that have to be overcome to make this work," he said. The Pentagon building, for example, is still relying on its host of legacy identification badges because of certain visual features not included on the CAC. Carey said security officials there would not be able to read that information from the CAC's magnetic strip, which could only allow general access to the building.

"We have to come through some issues on how do we make sure the guys walking the hallway are supposed to be there," he said. "The question is how much checking [to do] at the perimeter" vs. inside the building.

"We are working with the Pentagon's Force Protection Agency to create and figure out [how] to use [the current CAC], as well as the next-generation CAC because that has technologies that facilitate a higher level of security," Carey said.

Carey said wireless communication devices might play a role with future CACs. The card could eventually be used to access such devices; in turn, the devices may be used to identify a person by their CAC. For example, if someone is unrecognized in a restricted area, security officials could plug the person's card into a wireless communication device and access a personnel database to determine whether the person is properly authorized.